World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:1, No:10, 2007

A Copyright Protection Scheme for Color Images using Secret Sharing and Wavelet Transform

Shang-Lin Hsieh, Lung-Yao Hsu, and I-Ju Tsai

Open Science Index, Computer and Information Engineering Vol:1, No:10, 2007 publications.waset.org/2813/pdf

***Abstract*—** This paper proposes a copyright protection scheme for color images using secret sharing and wavelet transform. The scheme contains two phases: the *share image generation* phase and the *watermark retrieval* phase. In the *generation* phase, the proposed scheme first converts the image into the YCbCr color space and creates a special sampling plane from the color space. Next, the scheme extracts the features from the sampling plane using the discrete wavelet transform. Then, the scheme employs the features and the watermark to generate a principal share image. In the *retrieval* phase, an expanded watermark is first reconstructed using the features of the suspect image and the principal share image. Next, the scheme reduces the additional noise to obtain the recovered watermark, which is then verified against the original watermark to examine the copyright.

The experimental results show that the proposed scheme can resist several attacks such as JPEG compression, blurring, sharpening, noise addition, and cropping. The accuracy rates are all higher than 97%.

***Keywords*—**Color image, copyright protection, discrete wavelet transform, secret sharing, watermarking.

I. Introduction

THE rapid evolution of the Internet technology makes the transmission of digital multimedia contents easier nowadays than before. Copyrighted digital media such as images, music, etc, can be copied or distributed quickly and easily on the Internet. Media content owners are very concerned about the potential loss of revenue resulting from digital media piracy. Therefore, digital watermarking techniques have been proposed for copyright protection [1]-[4] or ownership identification of digital media.

Digital watermarking [4]-[8] is a technique used to protect the digital media property. Digital watermarking embeds a watermark into the host image. Later, it extracts the watermark from the suspected image for verification.

A watermark can be embedded in the spatial domain or the frequency domain. In the spatial domain, the watermark is embedded by changing the pixel values directly. In the frequency domain, the pixel values are transformed to frequency coefficients and the watermark is then embedded by modifying the coefficients. Generally, the robustness of the watermark embedded in the spatial domain is often weaker than that in the frequency domain.

The problem with both of the above watermarking techniques is that they modify some pixels of the host image directly or indirectly, which decreases the image quality. In addition, both of the techniques perform poorly when noise is added to the image.

To preserve the image quality, some researches looked for the techniques that do not alter the original image. Chang and Chuang [2] applied the visual secret sharing scheme (VSS) on the watermark to generate two share images and store one of them for later verification. In the verification phase, their scheme generates the other share image and superimposes the stored one on the generated one to retrieve the watermark. The problem with the scheme, however, is that its performance deteriorates as the JPEG compression ratio increases. Moreover, it only deals with gray-level images and does not consider color images.

In general, a color image can provide more perceptual information, i.e., sufficient evidence, against any illegal copyright invasion. However, in the past few years, most researches focused on developing watermarking schemes for gray-level images. Only a comparatively small number of researches on color image watermarking can be found [8]. Moreover, they all modify the host image.

The author once proposed a scheme [1] to protect copyright for gray-level images using secret sharing. In this paper, we extend the original scheme for color images and make some modifications to further improve the performance. To deal with color images instead of gray-level ones, the newly proposed scheme uses a specific sampling method to generate a sampling plane from the image and then extracts the features from the plane.

The proposed scheme has the following advantages. First, it does not modify the host image. Therefore, it is suitable for the application in which the modification of the image is not allowed. For example, satellite images cannot allow any modification on them because that will affect their precisions. Second, the scheme is secure. By applying the technique of secret sharing, only the user who has the share image can retrieve the watermark. Last, the scheme is robust. The experimental results show the scheme can resist five kinds of

Manuscript received on November 15, 2005.

The authors are with the Department of Computer Science and Engineering, Tatung University, Taipei, Taiwan (corresponding e-mail: slhsieh@ttu.edu.tw).

Open Science Index, Computer and Information Engineering Vol:1, No:10, 2007 publications.waset.org/2813/pdf

common image processing operations, including JPEG compression, blurring, sharpening, varied noise addition, and cropping.

The organization of the paper is as follows. Section II describes the related background of the proposed scheme. Section III explains the proposed sampling method. Section IV details the proposed copyright protection scheme. Section V examines the experimental results. Finally, section VI states the conclusion.

II. Related Background

The proposed scheme uses discrete wavelet transform (DWT), color image sampling, and secret sharing. This section briefly explains the above techniques.

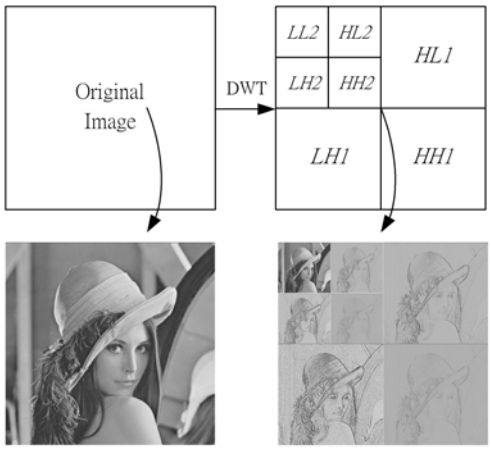


Fig. 1 Two-level DWT decomposition of Lena

A. Discrete Wavelet Transform

The basic idea of the DWT for an image is described as follows. An image is first decomposed into four sub-bands LL1, LH1, HL1, and HH1. The LL1 sub-band can be further decomposed into four sub-bands LL2, LH2, HL2, and HH2. The same decomposition procedure can be applied until there is only one coefficient in the LL sub-band. Fig. 1 shows the image "Lena" and the result after two-level DWT decomposition.

B. Color Image Sampling

There are different kinds of color image sampling. The following section describes the traditional 4:2:2 sampling.

Initially, the original image X is converted to the YCbCr color space. Equation (1) is the formula of YCbCr transformation according to CCIR Rec.601-1. The Y component represents the luminance. The Cb and Cr components represent the chrominance. Fig. 2 shows graphically the structure of the 4:2:2 sampling. Only two lines and 4 picture elements or "pixels" per line are shown in the figure. For the first pixel, the Y, Cb, and Cr components are sampled. For the second pixel, only the Y component is sampled. For the third pixel, Y, Cb, and Cr components are once again sampled and then for the fourth pixel, only the Y component is sampled. Therefore, there are four Y samples for every two Cr and Cb samples in a line, resulting in a ratio of 4:2:2. The above sampling rule is observed in other lines.

$$
\begin{aligned}
&RGB \rightarrow YC_bC_r \\
&Y = 0.2989 \times \mathrm{R} + 0.5866 \times G + 0.1145 \times B \\
&C_b = -0.1687 \times \mathrm{R} - 0.3312 \times G + 0.5000 \times B \\
&C_r = 0.5000 \times \mathrm{R} - 0.4183 \times G - 0.0816 \times B
\end{aligned}
\tag{1}
$$

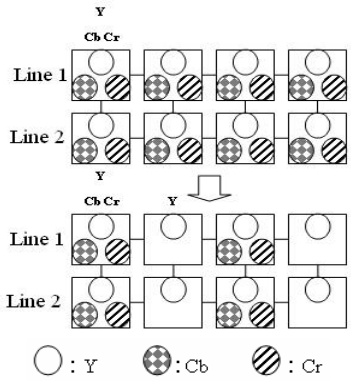


Fig. 2 The traditional 4:2:2 sampling

C. Secret Sharing

The proposed scheme applies the secret sharing scheme [11] [12] to protect image copyright. The secret sharing scheme splits an image into n different shares. The image can be retrieved with more than k ($k \leq n$) shares. The size of the retrieved image is expanded because each pixel is mapped into a block consisting of several sub-pixels. The effect is called *pixel-expansion*. Fig. 3 shows an example of the secret sharing scheme. Fig. 3(a) is the original image. Fig. 3(b) and 3(c) are the share images produced from the original one. Fig. 3(d) is the retrieved image, which contains the information that can be recognized visually with the human eyes. Note, the retrieved image is four times larger than the original one and contains noise.

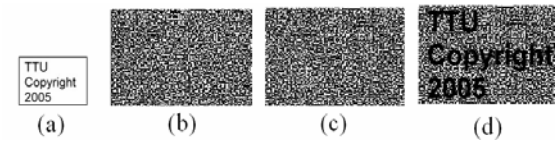


Fig. 3 An example of the secret sharing scheme; (a) the original image; (b), (c) the share images; (d) the retrieved image

III. The Proposed Samplinfg Method

The proposed scheme converts the image from the RGB color space into the YCbCr color space before feature extraction. Because experimentally the features extracted from the result of the traditional 4:2:2 sampling are not robust enough, the proposed scheme uses a specific sampling method for feature extraction. This section explains the proposed

Open Science Index, Computer and Information Engineering Vol:1, No:10, 2007 publications.waset.org/2813/pdf

sampling method.

A. The Rule of the Proposed Sampling Method

Fig. 4 shows a block of size 8 × 8 before and after sampling. There are eight pixels per line. The YCbCr components are sampled as follows.

1. The Y component is sampled for the first pixel to the fourth pixel.
2. The Cb component is sampled for the fifth pixel and the sixth pixel.
3. The Cr component is sampled for the seventh pixel and the eighth pixel.

In the other lines, Y, Cb, and Cr components are once again sampled according to the above rule.

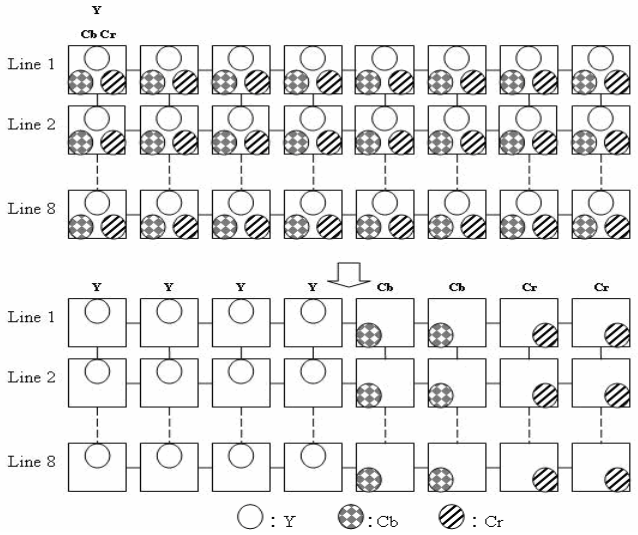


Fig. 4 The proposed sampling method

B. The Consideration of the Proposed Sampling Method

The arrangement of the proposed method can be described from another point of view as follows. The original image is divided into two interlaced images. The Y components are from one interlaced image and CbCr component are from the other interlaced image.

Because Y components and CbCr components are from two different interlaced images, an attack that affects the Y components will not affect the CbCr components, and vice versa.

IV. The Proposed Copyright Protection Scheme

The proposed scheme contains two phases: *share image generation* phase and *watermark retrieval* phase. Fig. 5 shows the block diagram of the proposed scheme. The *YCbCr feature extraction* in the *share image generation* phase first converts the color space from RGB into YCbCr. Then, it creates a sampling plane using the proposed sampling method and extracts the features from the sampling plane. Afterward, the *watermark scrambling* disarranges the watermark with a secret key. Finally, the *encoding* uses the features and the scrambled watermark to generate the principal share image, which is saved and will be used for *watermark retrieval*. To retrieve the watermark, the *YCbCr feature extraction* in the *watermark retrieval* phase first converts the color space of the suspect image from RGB into YCbCr. Then, it creates a sampling plane and extracts the features. The *decoding* next uses the features and the previously saved principal share image to retrieve the scrambled watermark. Afterward, the *watermark unscrambling* rearranges the scrambled watermark. Finally, the watermark is reduced to obtain the recovered watermark. The recovered watermark is then used to verify the copyright.

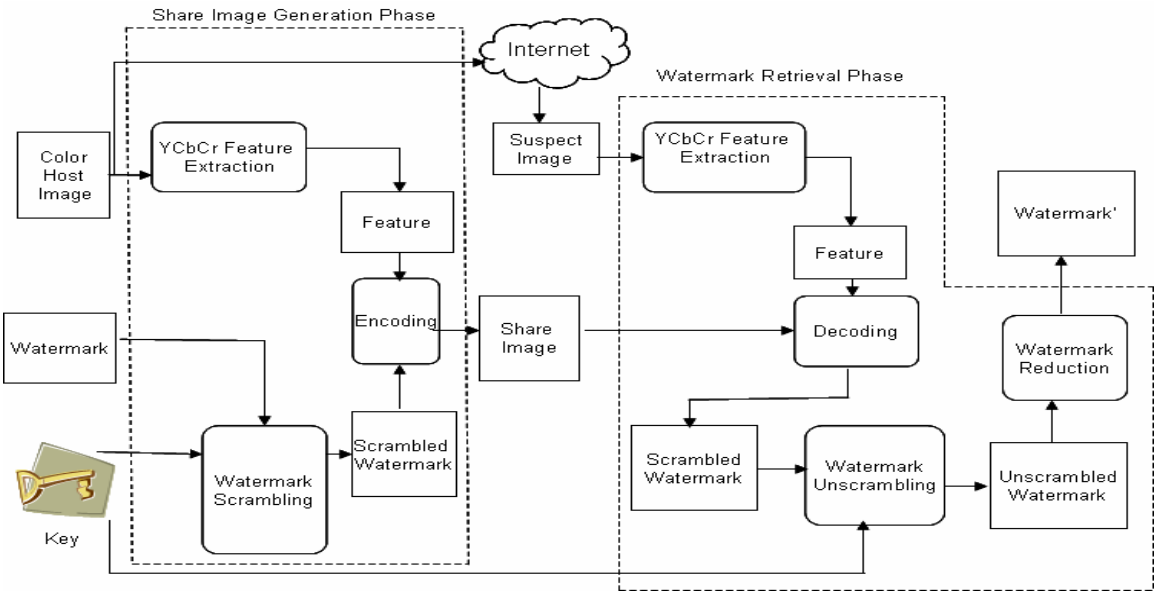


Fig. 5 The block diagram of the proposed scheme

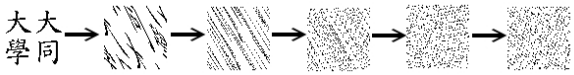


Fig. 6 The scrambled watermark

A. The Major Parts in the Proposed Scheme

There are four major parts in the scheme. The following subsections describe the details of the four parts.

1) Scrambling and Unscrambling Watermark

The proposed scheme uses Torus-automorphism [13] [14] to scramble the watermark in the *share image generation* phase and to unscramble the scrambled watermark in the *watermark retrieval* phase. Fig. 6 shows an example of a scrambled watermark after five iterations.

2) YCbCr Feature Extraction

Before feature extraction, the host and suspect images must be first converted to the YCbCr color space as described in Section II. Next, a sampling plane is generated from the YCbCr planes by the method described in Section III. Then, the sampling plane is divided into non-overlapping blocks of size 8×8 and the elements of each block are transformed to DWT coefficients.

After applying two-level DWT, there are four coefficients in the LL2 sub-band of each block. Let *M* be the average of the four coefficients. Then, *M* should satisfy one of the following conditions:

1. Only one coefficient is smaller than *M*.
2. Only two coefficients are smaller than *M*.
3. Only one coefficient is greater than *M*.
4. All of the four coefficients are the same and therefore equal to *M*.

A feature type is then obtained from the above rule. Let *n* be the feature type, which represents the number of the above conditions, then

$$n = \begin{cases} 1, \text{ if } M \text{ satisfy the condition (1)} \\ 2, \text{ if } M \text{ satisfy the condition (2)} \\ 3, \text{ if } M \text{ satisfy the condition (3)} \\ 4, \text{ if } M \text{ satisfy the condition (4)} \end{cases} \quad (2)$$

3) The Encoding and Decoding

According to the secret sharing scheme, two share blocks are created: principal share and complementary share blocks. Each of the two share blocks contains 2 × 2 pixels. Each pixel of the watermark can be mapped into a share block of 2 × 2 pixels according to the pixel value of the watermark. The share blocks form the share image.

Table I lists the mapping table used in the proposed scheme. A pixel of the watermark will be mapped into a block of size 2 × 2, which is called *pixel-expansion*.

The encoding process uses the extracted feature types and the watermark to generate the share blocks of the principal share image. The principal share blocks are generated according to the description in section IV.B.

The decoding process applies XOR operation (Table II) on the complementary share blocks obtained from the suspect image and the corresponding share blocks of the previously saved principal share image (generated from the original host image) to retrieve the scrambled watermark. Then, the scrambled watermark is unscrambled to obtain the visually recognizable watermark.

TABLE I
THE MAPPING TABLE FOR ENCODING AND DECODING

Feature Type n	Mean Value Location	The watermark pixel is white		P-Share XOR-C-Share	The watermark pixel is black		P-Share XOR C-Share
		P-Share	C-Share		P-Share	C-Share	
1	a<M< b,c,d						
	b<M< a,c,d						
	c<M< a,b,d						
	d<M< a,b,c						
2	a,b≤M<c,d						
	c,d≤M<a,b						
	a,d≤M<b,c						
	b,c≤M<a,d						
	a,c≤M<b,d						
	b,d≤M<a,c						
3	b,c,d≤M<a						
	a,c,d ≤M<b						
	a,b,d≤M<c						
	a,b,c≤M<d						
4	M=a=b=c=d						
	The four coefficients of the LL2 subband (a is at the top left, b is at the top right, c is at the bottom left, and d is at the bottom right position)						
P-Share: Principal share; C-Share: Complementary share							

Open Science Index, Computer and Information Engineering Vol:1, No:10, 2007 publications.waset.org/2813/pdf

Open Science Index, Computer and Information Engineering Vol:1, No:10, 2007 publications.waset.org/2813/pdf

TABLE II
THE XOR RULE

Pixel-1	Pixel-2	Pixel-1 XOR Pixel-2
■	□	□
□	■	□
■	■	■
□	□	■

4) Watermark Reduction

When the original watermark pixel is white, some redundant noise on the background of the unscrambled watermark will be generated due to the *pixel-expansion* effect of *secret sharing*. To regain the original watermark from the unscrambled watermark, a *watermark reduction* process is used to remove the redundant noise. According to the generated block by XOR, one of the following two steps will be adopted:

1. when the number of white pixels of the generated block is equal to 1 or 0, the block is reduced to a black pixel.
2. when the number of white pixels of the generated block is greater than 1, the block is reduced to a white pixel.

Table III lists the reduction conditions and the corresponding actions. Fig. 7 shows an example of a recovered watermark after reduction.

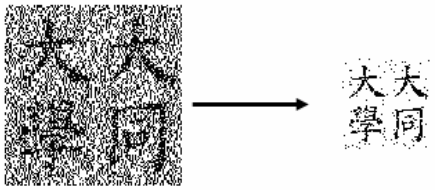
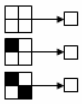


Fig. 7 The recovered watermark after reduction

TABLE III
THE REDUCTION CONDITION AND THE CORRESPONDING ACTION

Condition	Action	Condition	Action
The number of white pixels of the block is greater then 1	Reduce the result block into a white pixel	The number of white pixels of the block is equal to 1 or 0	Reduce the result block into a block pixel
	Example		Example
			

B. The Procedure of Share Image Generation

The *share image generation* phase first converts the color space of the host image from RGB into YCbCr. Next, it creates a sampling plane, from which it extracts the features. Then, it scrambles the watermark with a secret key. Finally, it generates the principal share image using the features and the scrambled watermark. The following lists the detailed steps.

Share Image Generation Procedure

Input: A color host image $H(N\times N)$, a watermark $W(N/8\times N/8)$, and a secret key for scrambling.

Output: The principal share image $S(N/4\times N/4)$ used to retrieve the watermark.

Step 1 Use Torus-automorphism and the secret key to scramble the watermark W into W'.

Step 2 Convert the color host image H into the YCbCr color space.

Step 3 Sample the color space to generate the sampling plane F according to the rule in Section III.

Step 4 Divide the sampling plane F into non-overlapping blocks of size 8×8 $F(k)$, k=1, 2, …, $N/8 \times N/8$, and divide the scrambled watermark W' into a binary digits sequence $W'(k)$, k=1,2,…, $N/8 \times N/8$.

Step 5 Let k be 1.

Step 5.1 Transform the sampling plane block $F(k)$ into four coefficients by two-level DWT decomposition.

Step 5.2 Calculate the average M of the four coefficients.

Step 5.3 Obtain the feature type n according to (2).

Step 5.4 Based on Table I, use the feature type n, the location of average M of the four coefficients, and the pixels of the corresponding scrambled watermark block $W'(k)$ to generate the principal share block $S(k)$.

Step 5.5 Increase k by one. If $k \le N/8 \times N/8$ go to Step 5.1.

Step 6 Output the principal share image S consisting of the share blocks.

The generated principal share image S is then saved and will be used in the *watermark retrieval* phase

C. The Procedure of Watermark Retrieval

The *watermark retrieval* phase first converts the color space of the suspect image from RGB into YCbCr. Next, it creates a sampling plane, from which it extracts the features. Then, it uses the features and the previously saved principal share image to retrieve the scrambled watermark. Finally, it rearranges the scrambled watermark and reduces the watermark to obtain the recovered watermark. The following lists the detailed steps.

Watermark Retrieval Procedure

Input: A color suspect image $H'(N \times N)$, the principal share image $S(N/4\times N/4)$, and the secret key for unscrambling.

Output: The recovered watermark $WR(N/8\times N/8)$

Step 1 Convert the color suspect image H' into YCbCr color space.

Step 2 Sample the color space to generate the sampling plane F'.

Step 3 Divide the sampling plane F' into non-overlapping blocks of size 8×8 $F'(k)$, k=1, 2, …, $N/8 \times N/8$, and divide the principal share image S into non-overlapping

Open Science Index, Computer and Information Engineering Vol:1, No:10, 2007 publications.waset.org/2813/pdf

blocks of size 2 × 2 $S(k)$, k=1,2,…, $N/8 \times N/8$.

Step 4 Let k be 1.

Step 4.1 Transform the sampling plane block $F'(k)$ into four coefficients by two-level DWT decomposition.

Step 4.2 Calculate the average M of the four coefficients.

Step 4.3 Obtain feature type n according to (2).

Step 4.4 Based on Table I, use the feature type n, and the location of average M of the four coefficients to generate the complementary share block $S'(k)$.

Step 4.5 Apply XOR operation on the complementary share block $S'(k)$ and the principal share block $S(k)$ to produce the corresponding scrambled watermark $W'(k)$.

Step 4.6 Increase k by one. If $k \le N/8 \times N/8$ go to Step 4.1.

Step 5 Use Torus-automorphism and the secret key to unscramble the watermark W' to W''.

Step 6 Use Watermark reduction process described in Section IV.A.4 to reduce the unscrambled watermark W'' and remove the noise to obtain the recovered watermark WR.

V. Experiments

We conducted some experiments to evaluate the feasibility of the proposed scheme. Fig. 8 shows the 256-color host image. Fig. 9 shows the watermark and generated principal share image. We used a commercial image processing software, Ulead PhotoImpact 8.0, to simulate different kind of attacks, including JEPG compression, blurring, sharpening, scaling, and varied noise addition.

The *Accuracy Rate* (*AR*) is used to measure the difference between the original watermark and the recovered one. *AR* is defined as follows:

$$AR = \frac{CP}{NP}, \tag{3}$$

where *NP* is the number of pixels in the original watermark and *CP* is the number of correct pixels obtained by comparing the pixels of the original watermark with the corresponding ones of the recovered watermark. The more closely *AR* approaches one, the more closely the recovered watermark resembles the original one.

Table IV lists the experimental results. On the left of the table are the results generated from the proposed scheme while on the right are the ones generated using the author's previous scheme for gray-level images [1]. Although a scheme designed for gray-level images cannot be applied on color images directly, it is still applicable if we treat the Y component of a color image as a gray-level image.

The experiment shows the recovered watermarks can all be easily recognized after the attacks. It also shows the proposed scheme outperforms the previous one for each attack. The accuracy rates are all higher than 97%

In addition, a uniqueness experiment was conducted to check whether a different image would be mistaken for the original one. The features of various images should be different, so the recovered watermark from an image different from the original one should contain nothing more than noise.

Fig. 10 shows the test image "Tiffany" and the recovered watermark which is different from the original image "Lena". The accuracy rate of "Tiffany" is 0.3889. The recovered watermark contains no information about the original watermark.

VI. Conclusions

In this paper, we proposed a copyright protection scheme for color images using secret sharing and discrete wavelet transform (DWT). The scheme is suitable for color images. Furthermore, we still preserve the advantages of the previously proposed scheme, which are

(1) it does not modify the host image, and therefore is suitable for unchangeable images,

(2) it is secure because of the employment of secret sharing and Torus-automorphism transformation, and

(3) it is robust according to the experimental results, which shows the accuracy rates are all higher than 97%.

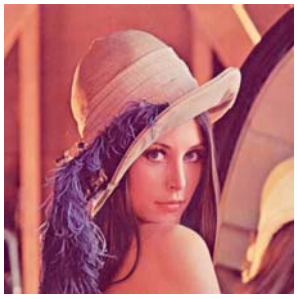


Fig. 8 The test color image "Lena" (512×512)

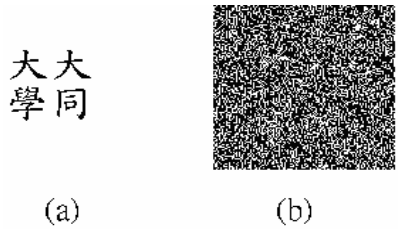
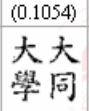


Fig. 9 (a) The watermark (64×64); (b) The principal share image (128×128)



Fig. 10 The test color image "Tiffany" and the recovered watermark

TABLE IV
EXPERIMENTAL RESULTS OF THE PROPOSED AND PREVIOUS SCHEMES

	The proposed scheme			The previous scheme		
JPEG	25%	50%	75%	25%	50%	75%
AR	0.9951 (0.0176)	0.9968 (0.0078)	0.9988 (0.0110)	0.9775	0.9890	0.9878
						
Blurring	5	3	1	5	3	1
AR	0.9761 (0.1729)	0.9822 (0.1480)	0.9939 (0.0676)	0.8032	0.8342	0.9263
						
Sharpening	5	3	1	5	3	1
AR	0.9797 (0.1399)	0.9907 (0.1054)	0.9949 (0.0689)	0.8398	0.8853	0.9260
						
Scaling	64x64	128x128	256x256	64x64	128x128	256x256
AR	0.9766 (0.2049)	0.9907 (0.0991)	0.9980 (0.0539)	0.7717	0.8916	0.9441
						
Noise Addition	10	8	6	10	8	6
AR	0.9944 (0.0996)	0.9951 (0.0913)	0.9951 (0.0852)	0.8948	0.9038	0.9099
						

REFERENCES

[1] Shang-Lin Hsieh and Bin-Yuan Huang, "A Copyright Protection Scheme for Gray-Level Images Based on Image Secret Sharing and Wavelet Transformation," Proceedings of International Computer Symposium, 2004.

[2] C.C. Chang and J. C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," Pattern Reconition Letters, vol. 23, pp. 931-941, June 2002.

[3] Ren-Junn Hwang, "A Digital Image Copyright Protection Scheme Based on Visual Cryptography," Tamkang Journal of Science and Engineering, vol.3, No. 2, pp. 97-106,2000.

[4] San-Hwa Wu and Hsiu-Feng Lin, "A Non-Embedded Watermarking Scheme for Non-Distortion Digital Product Copyright Verification, "2004.

[5] Xiang Zhou, Xiaohui Duan and Daoxian Wang, "A Semi-Fragile Watermark for Image Authentication," Proceedings of the 10th International Multimedia Modelling Conference, 2004.

[6] Xiaoqiang Li and Xiangyang Xue, "Improved Robust Watermarking in DCT Domain for Color Image," Proceedings of the 12th International Conference on Advanced Information Networking and Network, 2004.

[7] Narges Ahmidi and Reza Safabakhsh, "A Novel DCT-based Approach for Secure Color Image Watermark," Proceedings of the International Conference on Information Technology, 2004.

[8] Chun-Hsien Chou and Tung-Lin Wu, "Embedding Color Watermarks in color Images," IEEE, 2004.

[9] D.J.Fleet and D.J.Heeger, "Embedding Invisible Information in Color Image," in proc.ICIP'97, pp.532-535, Oct. 1997.

[10] M. kutter, F.Jordan and F. Bossen, "Digital Signature of Color Images Using Amplitude Modulation, " in Storage and Retrieval for Image and Video Database V, SPIE, vol.3022.pp. 518-526,San Jose, Ca Febuary 8-14, 1997.

[11] Lukac, R.; Plataniotis, K.N., "A secret sharing scheme for image encryption", 46th International Symposium, pp. 549- 554, June 2004.

[12] M. Naor and A. Shamir, "Visual cryptography", Advances in Cryptology-EUROCRYPT'94, Lect. Notes in Comput. Sci. vol. 950, pp.1-12, 1995.

[13] G. Voyatzis and I. Pitas, "Applications of torus automorphisms in image watermarking," in Proc. Int. Conf. Image Processing (ICIP), vol. 3, Lausanne, Switzerland, Sept. 1996, pp. 237–240.

[14] Chin-Chen Chang, Ju-Yuan Hsiao and Chi-Lung Chiang, "An Image Copyright Protection Scheme Based on Torus Automorphism", First International Symposium on Cyber Worlds (CW'02) November 06 - 08, 2002.

Open Science Index, Computer and Information Engineering Vol:1, No:10, 2007 publications.waset.org/2813/pdf